DAVIC Digital Audio-Visual Council

Copy Control Framework

Taipei, Sep. 15-19, 1997

Classification: **Unclassified**

Distribution: **Unrestricted**

Doc No: GS-R105
Release: A
Date: October 29, 1997
Owner: Gene Itkis, Goren Eriksson
Writer: Yonatan Silver

"OUTSIDE COUNSEL'S EYES ONLY"

WB 00854

Table of Contents

1. Scope

Copy control relates to control of production, distribution and use of audio and/or video content (such as movies and music recordings.) It includes protection against unauthorized copying of content. It can also include parental control, play-once options, and related fields.

This document reviews the current status of copy control from various angles, and suggests the direction that DAVIC could take in providing a general inter-operable copy control framework.

This framework is specifically designed to encompass rather than conflict with the work of other existing bodies that are developing relevant standards.

The editors can be contacted at the following e-mail addresses:

Gene Itkis: itkis@ndsisrael.com

Goran Eriksson: goe@teracom.se

2. Background

2.1. WHY DO WE NEED COPY CONTROL?

Content Providers are losing significant amounts of potential profits to pirates. For example, here are some facts and figures provided by the International Federation of the Phonographic Industry (IFPI):

- Over $5 billion per year are lost to pirates by the music industry alone, and this does not include "home copying", (this number is obtained as "recording studios' revenues" minus "legitimate orders")
- In some South American countries the percentage of pirate music recordings in the market runs as high as over 90%.[1]
- The connection between CD piracy and organized crime has been demonstrated in some countries.

A similar situation is likely to be true for the video industry.

Piracy in the digital domain is a greater problem than that of the analog domain because:

- copies of digital content may be of the same quality as the original.
- distribution of digital material (e.g., over the internet) is much easier.
- the tools for digital copying are mostly software, and much easier to develop, use and distribute.

So, the purpose of copy control mechanisms is to maintain integrity of commerce systems, by ensuring that those involved in the creative process are compensated for their contributions (financial and intellectual) and encouraged to continue them. This should include ensuring that the consumers get what they pay for - no more and no less.

Creating a fair and competitive environment would benefit all the players.

[1] Action item: get the confirmed exact numbers from Paul Jessop (paul.jessop@ifpi.org)

2.2. PIRATES AND PIRACY

2.2.1. Types of Piracy

The following classification of piracy was suggested by IFPI and probably reflects the situation in other media and/or industries:

- **counterfeit:** A pirate copy that looks identical to the original.

  Such counterfeit CDs can, and have, been produced within a week from the official release.

- **simple/back-catalog:** Unauthorized compilations produced by pirates (without permission from the owners of rights to the material.)

  This type of piracy is especially lucrative and hard to enforce for older material, because it is not always known who owns the rights to old material.

- **bootlegging:** Illegal recordings of a live performance.

- **home copying:** Although this is not technically considered piracy, it is undesirable. It is therefore also included in the discussion below.

2.2.2. Piracy of Media vs. Players

In the past pirates have copied the media. It the context of Pay-TV, pirates have also produced or modified equipment to obtain services without authorization.

It is possible that in the future both these types of piracy will be relevant to copy control.

Player piracy is generally more difficult and expensive for pirates because this involves developing or modifying expensive equipment. Such modifications would generally void manufacturer warrantees and services, and would therefore not be popular with the pirates' clientele.

2.2.3. Pirates: From Professional to Casual

One way of classifying pirates is according to skill and access to equipment:

a. Highly skilled, well-financed and well-equipped[2] organizations;

b. Fairly sophisticated (groups of collaborating) individuals, such as students.

   Typically such pirates have little more than a PC and some simple electronics available to them. They may also have access to some university facilities.

c. Casual (relatively unsophisticated) users who are prepared to violate the law, but are able perform the piracy only if the necessary (simple) equipment and (straight-forward) instructions are made available to them.

[2] In some cases they have access to laboratories equipped with electronic microscopes and similar equipment.

The above list represents points on a continuous spectrum of various possible types of pirate activity. The distinctions between the different types of pirates may often shift or be blurred.

An alternative classification of piracy is based on the pirates' motivation. The *professional* pirates make money from their activity, as opposed to *amateur* pirates who act for their personal pleasure.

For example, an amateur pirate may produce a (*free*) copy for himself and a few friends, while the professional pirate will *sell* as many copies as she can.

In reality, these distinctions are not always clear, with some amateur pirates asking their friends for small (cost-covering) fees and possibly growing into the small-scale extra-income business.

The importance of the professional-amateur distinction is also not clear. Some Content Providers are mainly concerned with professional piracy, while others (including those in the very same industry) are worried mostly about losses of revenue due to activities by amateurs.

2.3. HOW MUCH PROTECTION IS "ENOUGH"?

There has been a tendency to divide the pirates into two vaguely defined groups (as discussed earlier). Reflecting the vagueness and confusion behind this division, these groups are often referred to as casual and professional pirates.

Also, reflecting the difficulty in defending against professional piracy, there has been a tendency to advocate only a limited defense, i.e., only against casual piracy.

As has been evident in similar technologies, there is a viable migration path between professional to casual piracy[3] : amateurs may become professional; and tools and information previously available to professionals may become available to amateurs. It is furthermore our estimation that this type of migration is likely to become easier and more commonplace with the proliferation of PCs, the Internet and associated tools and services.

So, it appears more prudent to assume that copy control mechanisms not addressing professional pirates, are likely to quickly become inadequate even for copy control against casual pirates.

It is generally accepted that 100% security is unlikely to be achieved. Therefore, the aim of good security is to, at least, make piracy financially unattractive: ideally, a pirate copy should end up costing more than a legitimate one.[4]

Reliable numbers required to estimate a good/reasonable cut-off point are generally unavailable. It is difficult to estimate in advance the pirates' costs; both for development of a system to violate copy control mechanisms, and the distribution costs of the pirated

[3] A specific example has been seen in the pay-TV business where a system hack had been developed at first by the professional pirates. Then, within a very short time amateur pirates developed a hack of the professional pirate system. This hack was then posted to the Internet, making it available to the casual pirates.

[4] This criteria is hard to evaluate for back-catalog and bootleg piracy since no identical legitimate copies are available. The notion of the "added value" provided by the pirate and its cost should be estimated in order to provide a reasonable cut-off point for "good-enough" control (i.e., raising the pirates' costs high enough to minimize/eliminate their profit margins).

materials/services. Therefore, this decision is generally made on the basis of speculation and ungrounded assertions.

The present situation is further complicated by the fact that the Content Providers (CP)-- who are the proper judges of how much security is enough -- can exhort only (political) pressure on the Consumer Electronics manufacturers (CE)-- who must spend their resources to implement the solution for which they get no direct benefit.

Therefore, the CE have to be motivated to do the best job possible. It would only be fair to provide them with adequate compensation for supporting the best solutions possible.

Ideally, it would be more natural if the Content Providers use their budgets to control the choice of the security mechanisms/levels, balanced by the cost of implementing them. The CE in this ideal situation would view a CP as a customer paying for the implementation of the specified mechanisms.

Currently, Content Providers typically subcontract the provision of security mechanisms/levels to Conditional Access/Security Providers (CA).

One of the goals of the framework advocated in this document is to make this business model restructuring possible. This will be discussed in greater detail later.

2.4. CURRENT COPY-CONTROL MECHANISMS

2.4.1. Techniques

Current copy-control techniques, and, specifically, responses to DAVIC CFP7, include encryption, data hiding (watermarking), and digital signatures. The potential of these techniques were evaluated in the baseline 85 and
CFP7-011.

- Encryption is typically employed to make the content unavailable to illegitimate users. However, by pretending to be a legitimate user, a pirate can obtain the content. To copy the content, the pirate needs to tap into the data path from the encrypted content to the played out content. Finding the most convenient place for this tap which will provide a high quality signal may present some degree of challenge to the pirate, but does not seem to be an intrinsically difficult task. In addition, the pirate generally needs to expend the financial and technical resources required to solve this problem only once to obtain all content encrypted in the same manner.

- Cryptographic/digital signatures can be used to guarantee the integrity of the content and associate a proper authorization with the specific content. This method does not, however, address the issue of ensuring enforcement of the authorizations.

- Watermarking resiliently embeds data in content. This can be used to:

  a. prevent illegitimate copies from being recorded and/or played.

     In this case, the requirement placed on the watermark is that it can be read/verified by every legitimate player/recorder. But, at the same time, it is essential that the pirates can neither obliterate nor change the watermark. Because the watermark-reading mechanism is to be present in every legitimate player, it is reasonable to

expect that the pirates will eventually discover all the secrets required for reading these watermarks. Developing watermarks, which the pirate knows how to read but does not know how to modify or remove, appears to be an inherently very difficult, and, some experts believe, even impossible problem.

b. mark specific content so it can be easily identified by its owner, and possibly allow the ownership to be proven in court.

Here, the requirements placed on the watermarks are much weaker and many watermark technologies are well suited to satisfy them.

2.4.2. Copy vs. Playback Control

There are two distinct approaches to provision of Copy Control.

- Prevention of production of unauthorized copies (for example, CCI copy bits.)
- Prevention of playback of unauthorized copies.

It is widely believed that everything that can be seen can be copied. This would appear to suggest that the emphasis for Copy Control should be on the second approach.

2.4.3. Defenses Provided

We can consider three types of defenses provided by the above mentioned techniques:

1. Authorizations

For example, copy bits (CCI). These can be supported by either the cryptographic strength of the digital signatures or the integrity of the watermarks.

2. Content inaccessibility for illegitimate use

This can be supported by the encryption techniques.

3. Off-line measures

For example, law enforcement. This can be supported by the second use of the watermarks described earlier.

The effectiveness of the second approach is likely to be limited, as argued above. While the off-line measures can be very effectively supported even with the existing technologies, the scope of application of these measures is unfortunately rather restricted. So, it is our belief that while all three methods have important roles to play, the authorization-based approach appears to be the best choice for the main focus. The other methods should perhaps be best viewed as a means of enforcing the authorizations.

3. Looking Ahead

3.1. LEGAL APROACHES

Copy control mechanisms can have different level of reliance on the legal mechanism. There are two components to such legal mechanisms:

- legislation; and
- law enforcement.

While the value of the legal means of enforcing copy control should not be ignored, we should be very careful in evaluating its effectiveness (which should also be done on a case by case basis).

In particular, different countries have very different laws and legal systems.[5] At the same time, even when appropriate laws are in place, the effective enforcement of these laws is often either difficult or non-existent. Semi-anecdotal evidence is provided by the editors who are aware of examples of illegal cable boxes being distributed in New York by a policeman or a legitimate TV store salespeople in Sweden[6] advising customers against purchasing legitimate services and directing them to the black market.

The high cost of law enforcement can be illustrated by the pay-TV industry's cases which dragged through the courts for years without reaching conclusions. It is also very likely that as the pirate industry matures it will make sure to isolate and protect the more important part of their infrastructure, leaving only the lowest level distributors vulnerable to law enforcement actions.

The proliferation of computers and the Internet is likely to make it particularly easy for pirates to lower the effectiveness of law enforcement directed against them.

[5] This problem has been exposed in the negotiations between China and the USA.

[6] It is interesting to note that Sweden is perceived to be particularly aggressive in its law enforcement against this type of piracy.

3.2. BUSINESS APPROACHES

Compared to the other similar models, the business model for copy control is not very well developed.

The Pay-TV Model

For example, in the case of pay-TV the grossly oversimplified model looks as follows: the Content Providers contract Conditional Access companies to provide the piracy prevention. The Content Providers have full control over the level and types of security they want delivered. Conditional Access companies strive to provide better services and security than the competition. Conditional Access companies may, in turn, subcontract elements of implementation of their security solutions to electronics manufacturers.

Everyone is this model is paid for the services they provide and is therefore motivated to provide the best service possible. Contractors for services are free to choose the type and level of service they require to meet their requirements and budget.

Current Copy-Control Model

In contrast, in the situation of copy control the Content Providers apply only "political" pressure on the Consumer Electronics industry; and the Consumer Electronics industry is not compensated for the solutions they provide at their own expense on a goodwill basis.

The elements that make the Pay-TV model to work are absent from the Copy-Control model. Competition and compensation for services provided are completely missing.

Objective

We believe it is a worthy goal to try to create a business model replacing the "political" pressures with contractual responsibilities and freedom of choice and competition. Such a model should include:

- Giving full control over the security choices to the Content Providers (who are the beneficiaries from the security and therefore should be the ones to determine what security is required);
- Creating a Security Provider role. These will be chosen and paid by the Content Providers and will be responsible for implementing security;
- Compensating the CE industry for implementing the security mechanisms to the specifications provided to them by the Security Provider.

3.3. INTERFACE WITH OTHER STANDARDS BODIES

A number of forums and standards dealing with copy control exist for various media and industries. Examples include CPTWG (dealing mainly with the DVD), VHS and Macrovision (for analog video), and others. A newer and less industry/media specific body to deal with copy control is MPEG-4. As new media appear, new standards are likely to evolve. Presently, there is no general framework that addresses all aspects and standards relating to copy control.

At some point the DAVIC Security TC had hoped that CPTWG, which has very strong industry backing and participation of the important players, would develop some solutions that DAVIC would be able to adopt.

It now appears that CPTWG's declared focus may be too narrow to be adopted by DAVIC. Namely, the solutions are specifically directed to the DVD market, are rather short term (i.e., not intended to provide security for any extended period - only for this generation of the players) and focus only on casual copying.

Since DAVIC focuses on a more global end-to-end system view in the area of copy control, it should also focus on wider, more general, and longer range solutions. We also argued above that it is highly preferable to focus on the professional rather than casual piracy.

Incorporating Standards in the Copy-Control Framework

The current standards are each relevant within their specific domain.

It is envisaged that the copy-control framework to be developed would provide the interface into which all relevant current and future standards could be incorporated.

In addition to formulating the framework, mechanisms for interfacing with existing and future standards (committees) should be developed. This is described in greater detail in the next section.

3.4. FRAMEWORK/INTERFACES VS. SPECIFIC SOLUTIONS

It is highly improbable that a single long-lasting solution common to all existing and future technologies will/can be developed.

It is therefore our suggestion that the focus for DAVIC should be on developing a framework and the interfaces which would allow short-lived and technology specific solutions to be integrated to provide a stable long-range general copy control.

Thus, DAVIC would develop a logical structure of authorizations and leave their enforcement and security maintenance details to the technology-specific methods.

One of the aspects of this structure that becomes obvious is possibility to provide and support "delegation of responsibility" from one entity to another (such a mechanism is described in CFP7-011).

Each such "delegation of responsibility" may be accompanied by a set of conditions. This type of flexible logical structure can potentially support a much greater range of business models and scenarios than can be easily anticipated otherwise[7].

Further requirements may be expected from the business community outside DAVIC once the benefit of the authorization structure is realized, thus potentially adding to the attractiveness and value of DAVIC.

It is therefore proposed that DAVIC undertake the mission of developing a standardized flexible authorization structure across technological platforms.

[7] Therefore, it may affect the DAVIC baseline document #84 which describes the copy-control information structure.

4. Conclusion

We have advocated the development of a general framework which will integrate all technology-specific solutions into a single system for copy control.

Such a framework will support and encourage a business model that will facilitate the development, maintenance and support of flexible and powerful copy-control mechanisms.

The framework should focus on authorization. Technology-specific solutions, as well as techniques such as digital signatures, encryption, and watermarking can be used for the implementation/enforcement of the authorizations.

Some features which can be realized within this approach have been illustrated in CFP7-011. This document goes even further and describes the Copy-Control Framework based on explicit and well structured authorizations.

The Copy-Control Framework provides the interface into which all relevant current and future standards could be incorporated.

By adopting and developing such a framework, DAVIC would be able to provide the opportunities and environment conducive to more powerful and flexible business support.

5. Acknowledgments

The editors would like to thank Mr. Paul Jessop of IFPI for his valuable help.

6. References

- DAVIC CFP7
- DAVIC CFP7-011
- DAVIC Baseline #84
- DAVIC Baseline #85